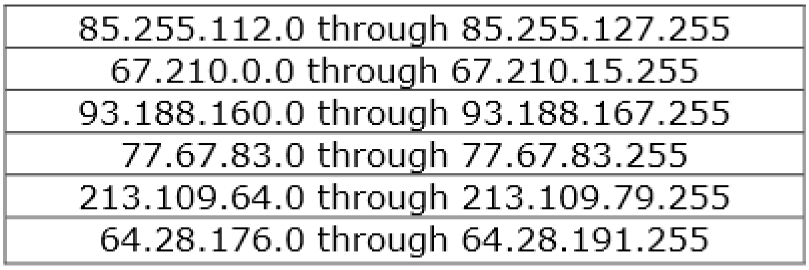
DNS

What is DNS: http://en.wikipedia.org/wiki/Domain_Name_System

Provider	Primary DNS Server	Secondary DNS Server
Level3	209.244.0.3	209.244.0.4
Google	8.8.8.8	8.8.4.4
Comodo Secure DNS	8.26.56.26	8.20.247.20
OpenDNS Home	208.67.222.222	208.67.220.220
DNS Advantage	156.154.70.1	156.154.71.1
Norton ConnectSafe	199.85.126.10	199.85.127.10
GreenTeamDNS	81.218.119.11	209.88.198.133
SafeDNS	195.46.39.39	195.46.39.40
OpenNIC	216.87.84.211	23.90.4.6
Public-Root	199.5.157.131	208.71.35.137
SmartViper	208.76.50.50	208.76.51.51
Dyn	216.146.35.35	216.146.36.36
FreeDNS	37.235.1.174	37.235.1.177
censurfridns.dk	91.239.100.100	89.233.43.71
DNS.WATCH	84.200.69.80	84.200.70.40
Hurricane Electric	74.82.42.42	
puntCAT	109.69.8.51	
More DNS	http://public-dns.tk/	

Read about: DNSChanger Malware

Rogue DNS Servers or bad DNS servers:



85.255.112.0 through 85.255.127.255
67.210.0.0 through 67.210.15.255
93.188.160.0 through 93.188.167.255
77.67.83.0 through 77.67.83.255
213.109.64.0 through 213.109.79.255
64.28.176.0 through 64.28.191.255

Which content filtering policies are available for home and personal use?

The following three pre-defined content filtering policies are available for home and personal use:

Policy 1: Security (199.85.126.10 and 199.85.127.10) This policy blocks all sites hosting malware, phishing sites, and scam sites. To use Policy 1, you should configure the DNS settings of your home router or Web-enabled device to use the following Norton ConnectSafe IP addresses: **199.85.126.10** and **199.85.127.10**.

Policy 2: Security + Pornography (199.85.126.20 and 199.85.127.20) In addition to blocking unsafe sites, this policy also blocks access to sites that contain sexually explicit material. To use Policy 2, you should configure the DNS settings of your home router or Web-enabled device to use the following Norton ConnectSafe IP addresses: **199.85.126.20** and **199.85.127.20**.

Policy 3: Security + Pornography + Other (199.85.126.30 and 199.85.127.30) In addition to blocking unsafe sites and pornography sites, this policy also blocks access to sites that feature mature content, abortion, alcohol, crime, cults, drugs, gambling, hate, sexual orientation, suicide, tobacco or violence. To use Policy 3, you should configure the DNS settings of your home router or Web-enabled device to use the following Norton ConnectSafe IP addresses: **199.85.126.30** and **199.85.127.30**.

Change Yours DNS on Yours device:

https://support.hidemyass.com/hc/en-us/articles/202720776-Changing-your-DNS-settings-on-Windows-Mac-Android-iOS

The best “open” DNS

censurfridns.dk

This page contains a list of frequently asked questions and answers. More might be added over time.

- Q: Why create www.censurfridns.dk ? Why run uncensored DNS Servers ?
- A: I am strongly against using DNS as a tool to filter content on the internet. Many people do not have the technical know-how to setup their own DNS server, so I created http://www.censurfridns.dk so there is a danish uncensored alternative to the internet providers filtered DNS servers.
- Q: Why not just use OpenDNS or Google DNS ?
- A: OpenDNS sucks, see why. As for Google DNS, well I just don't really like the idea of them receiving every DNS query I make.
- Q: Do ns1.censurfridns.dk and ns2.censurfridns.dk log any personal information ?
- A: Absolutely nothing is being logged, neither about the users nor the usage of this service. I do keep graphs of the total number of queries, but no personally identifiable information is saved. The data that is saved will never be sold or used for anything except capacity planning of the service.
- Q: Where are the servers located ?
- A: The servers are physically located in Denmark. They are placed on fast uplinks in professional data centers. The IP addresses will never change if I can prevent it.
- Q: Who is behind this service ?
- A: My name is Thomas Steen Rasmussen. I operate this DNS service as an individual with my own money. Questions and comments to admin@censurfridns.dk please.